Atlas (https://cloud.mongodb.com/v2#/org/66484beaf50dc267913cff01/) (https://cloud.mongodb.com/v2#/org/66484beaf50dc267913) Access Manager

Edit User: coffee-SHOP-bd-89124@admin

Update a database user to grant an application or user access to databases and collections in your clusters in this Atlas project. Granular access control can be configured with default privileges or custom roles. You can grant access to an Atlas project or organization using the corresponding Access Manager

Authentication Method

Password | Certificate | AWS IAM (MongoDB 4.4 and up) | Federated Auth (MongoDB 7.0 and up) PREVIEW

coffee-SHOP-bd-89124

xjr1B8CSxqDSJuWA HIDE

Autogenerate Secure Password | Copy

Database User Privileges

Configure role based access control by assigning database user a mix of one built-in role, multiple custom roles, and multiple specific privileges. A user will gain access to all actions within the roles assigned to them, not just the actions those roles share in common. **You must choose at least one role or privilege.** Learn more about roles. (https://docs.mongodb.com/manual/core/authorization/)

Built-in Role

1 SELECTED

Select one built-in role (https://docs.atlas.mongodb.com/security-add-mongodb-roles/#mongodb-roles) for this user.

Custom Roles

Select your pre-defined custom role(s). (https://docs.atlas.mongodb.com/security-add-mongodb-roles/#mongodb-roles) Create a custom role in the Custom Roles tab.

Specific Privileges

Select multiple privileges and what database and collection they are associated with. Leaving collection blank will grant this role for all collections in the database.

Restrict Access to Specific Clusters/Federated Database Instances /Stream Processing Instances

Edit User: coffee-SHOP-bd-89124@admin

Update a database user to grant an application or user access to databases and collections in your clusters in this Atlas project. Granular access control can be configured with default privileges or custom roles. You can grant access to an Atlas project or organization using the corresponding Access Manager

Authentication Method

Password	Certificate	AWS IAM (MongoDB 4.4 and up)	PREVIEW Federated Auth (MongoDB 7.0 and up)

(https://docs.mongodb.com/manual/core/security-scram-sha-1/)

Autogenerate Secure Password

Database User Privileges

Configure role based access control by assigning database user a mix of one built-in role, multiple custom roles, and multiple specific privileges. A user will gain access to all actions within the roles assigned to them, not just the actions those roles share in common. **You must choose at least one role or privilege.** Learn more about roles. (https://docs.mongodb.com/manual/core/authorization/)

Built-in Role 1 SELECTED

Select one built-in role (https://docs.atlas.mongodb.com/security-add-mongodb-roles/#mongodb-roles) for this user.

Custom Roles

Select your pre-defined custom role(s). (https://docs.atlas.mongodb.com/security-add-mongodb-roles/#mongodb-roles) Create a custom role in the Custom Roles tab.

Specific Privileges

Select multiple privileges and what database and collection they are associated with. Leaving collection blank will grant this role for all collections in the database.

Restrict Access to Specific Clusters/Federated Database Instances /Stream Processing Instances